REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address**: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): "THE FIRST SALVO: IMPLICATIONS OF STANDING RULES OF ENGAGEMENT FOR U.S. FORCES IN NETWORK-CENTRIC WARFARE" (U)	
9. Personal Authors: LCDR MICHAEL P. DONNELLY, USN	
10.Type of Report: Final	**11. Date of Report**: 4 FEBRUARY 2002
12.Page Count: 28	**12A. Paper Advisor:** CDR GREGORY J. O'BRIEN, JAGC, USN
13.Supplementary Notation: A PAPER SUBMITTED TO THE FACULTY OF THE NWC IN PARTIAL SATISFACTION OF THE REQUIREMENTS OF THE JMO DEPARTMENT. THE CONTENTS OF THIS PAPER REFLECT MY OWN PERSONAL VIEWS AND ARE NOT NECESSARILY ENDORSED BY THE NWC OR THE DEPARTMENT OF THE NAVY.	
14. Ten key words that relate to your paper: ROE, SROE, NCW, NETWORK-CENTRIC, ANTICIPATORY, STANDING, RULES, SELF-DEFENSE, PREEMPTIVE, INTENT.	

15.Abstract: Network-centric warfare (NCW) will create distinct advantages in the operational factors of space, time, force, and their interrelationships. Information superiority, the capability for cooperatively engaged precision effects, and a responsive command and control architecture will enable commanders operating in NCW to preempt enemy forces, negating an adversary's options before they can be executed. Though the technical challenges in NCW are significant, they are incrementally proving surmountable through war gaming and experimentation. The true limit of NCW's operational capability however, may not be technology, but law and politics.

Standing Rules of Engagement for U.S. Forces provides the base-line guidance and authorization for the use of military force in concert with international law and national policy. This paper examines the implications for NCW under Standing Rules of Engagement for self-defense, revealing several potential vulnerabilities and ambiguities that could significantly impact its operational capability. Operational concepts, structure, doctrine, and planning must anticipate the reality that military operations will be constrained by law and political imperatives.

Though NCW provides unprecedented levels of battlespace knowledge and speed of command, the initiative that it avails U.S. forces could be significantly undermined if it fails to adequately coalesce with rules of engagement (ROE).

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		**20.Office Symbol:** C	

(Unclassified Paper)

NAVAL WAR COLLEGE

Newport, R.I.

THE FIRST SALVO: IMPLICATIONS OF STANDING RULES OF ENGAGEMENT FOR U.S. FORCES IN NETWORK-CENTRIC WARFARE

by

Michael P. Donnelly
Lieutenant Commander, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

4 February 2002

Advisor: CDR Gregory J. O'Brien, JAGC, USN
Director, Maritime & Space Operations
International Law Department
Center for Naval Warfare Studies, NWC

Abstract

THE FIRST SALVO
IMPLICATIONS OF STANDING RULES OF ENGAGEMENT FOR U.S. FORCES IN NETWORK-CENTRIC WARFARE

Network-centric warfare (NCW) will create distinct advantages in the operational factors of space, time, force, and their interrelationships. Information superiority, the capability for cooperatively engaged precision effects, and a responsive command and control architecture will enable commanders operating in NCW to preempt enemy forces, negating an adversary's options before they can be executed. Though the technical challenges in NCW are significant, they are incrementally proving surmountable through war gaming and experimentation. The true limit of NCW's operational capability however, may not be technology, but law and politics.

Standing Rules of Engagement for U.S. Forces provides the base-line guidance and authorization for the use of military force in concert with international law and national policy. This paper examines the implications for NCW under Standing Rules of Engagement for self-defense, revealing several potential vulnerabilities and ambiguities that could significantly impact its operational capability. Operational concepts, structure, doctrine, and planning must anticipate the reality that military operations will be constrained by law and political imperatives.

Though NCW provides unprecedented levels of battlespace knowledge and speed of command, the initiative that it avails U.S. forces could be significantly undermined if it fails to adequately coalesce with rules of engagement (ROE).

TABLE OF CONTENTS

Joint Vision 2020 has identified information superiority, obtained through technologically advanced information operations, as a key enabler in future war-fighting operations.[1] Network-centric warfare (NCW) creates distinct advantages in the operational factors of space, time, and force by availing commanders the ability to achieve dominant battlespace knowledge[2] and massed effects from combined precision-fires. Higher levels of situational awareness, new structures and concepts of command, and the ability for cooperative and automated engagement of rapidly identified and determined targets will provide unique capabilities for U.S. forces. Yet, the initiative that NCW provides to U.S. forces could be minimized, or worse negated, if it fails to adequately coalesce with rules of engagement (ROE).

This paper will examine NCW with regard to the right of self-defense under current *Standing Rules of Engagement for U.S. Forces* (SROE)[3]. Specifically, two questions: (1) How will the changes in operational command and control that are inherent to NCW's theory of operation influence the effective use of force in self-defense under current SROE?; and, (2) What are the implications for NCW's capability of "taking early offensive and defensive actions,"[4] thus "stopping something before it starts?"[5] As operational capabilities change—particularly in the significance that NCW theorists predict—SROE must be evaluated to ensure that it still provides a sufficient relationship between its three principal foundations: national policy, operational capability, and law.[6] Likewise, the capabilities and evolving doctrine of NCW must be examined in light of international law and national policy to ensure maximum realization of its potential.

Defining rules of engagement. "ROE are the means by which the National Command Authorities (NCA)…express their intent as to how force will and will not be used

to achieve *policy* objectives."[7] As a measure of effectiveness, ROE must provide an adequate balance between national policy, operational requirements, and law.[8] Therefore, effective ROE provides the capacity—via constraints, restraints, and authorizations—for the effective use of military force within the bounds of law and in consideration of national policy.[9] In the absence of the direct control of forces, ROE is the apparatus by which the NCA ensures that the means can effectively achieve the end.

There are two distinct types of ROE: mission accomplishment ROE and self-defense ROE. SROE defines the self-defense ROE for U.S. forces. While SROE will rarely, if ever, serve as the sole guidance to forces in the conduct of their mission, it does serve as the basis for all U.S. specific mission accomplishment ROE.[10] By supplementing SROE, mission accomplishment ROE may provide authority for force—certain weapons or action—or restrict the use of force in order to ensure consistency between military means and political imperatives while accomplishing a specific mission.[11] While they may be more restrictive—providing specific procedures for the use of force or for distinguishing hostile forces—ROE supplemental measures can never negate the inherent right of self-defense provided under SROE.[12]

The distinction between self-defense and mission accomplishment ROE is important and necessary. "While ROE governing the use of force to accomplish the mission must be precise enough to safeguard against exceeding the policy mandate, falling short of it, or violating international law, self-defense rules are intentionally drafted broadly in order to pass as much discretion to the operator as possible…. Therefore, whereas mission accomplishment ROE should anticipate scenarios, self-defense ROE should clarify standards."[13]

Standing Rules of Engagement for U.S. Forces is founded in the legal interpretations, definitions, and precedence of *The Charter of the U.N.* As such, SROE identifies the conditions for the use of force in self-defense against armed attack, explicitly basing such authority in the elements of *necessity* and *proportionality* as defined within Article 51 of the U.N. Charter.[14] These two elements, essential to the right of self-defense, are well founded in international law.[15] (SROE is predicated on a cause and effect relationship with respect to the enemy, where proportionality and necessity define when and how force may be resorted to.)

Necessity in self-defense is defined as "the requirement that a use of force be in response to a hostile act or demonstration of hostile intent."[16] It is the realization of a hostile act or the determination of hostile intent that justifies the use of force—with regard to proportionality—in self-defense. A hostile act is distinguishable as an *actual* attack, or use of force, by an enemy.[17] Within the SROE, hostile act is defined as:

> An attack or other use of force by a foreign force against the United States, U.S. forces, and, in certain circumstances, U.S. nationals, their property, U.S. commercial assets, and/or other designated non-U.S. forces, foreign nationals and their property…[18]

While there is debate in international law as to the interpretation of "attack,"[19] the SROE definition provides a relatively clear context for commanders to determine such an occurrence.[20]

"Hostile intent," however, is as nebulous a term in SROE as it is in international law. Within SROE, hostile intent is defined as "the threat of imminent use of force by a foreign force or terrorist unit, or organization…."[21] Under SROE, determination of hostile intent provides justification for the use of force under the concept of anticipatory self-defense, thus allowing U.S. forces to *preempt* an adversary's *imminent* attack or use of force, within the

bounds of proportionality. The basis for anticipatory self-defense is that, in the face of perceived danger of attack, one should be allowed to take appropriate measures in self-defense[22]—such as Israel did in its preempted attack against Egypt during the 1967 Six Day War. However, the concept of anticipatory self-defense is a point of vast contention in the international community.[23] The argument of its opponents is that determinations of intent, by definition, are never certain.[24] (Thus, the potential strain on U.S. national policy for misinterpretations in the determination of necessity.)

"Even with definitional clarity, hostile intent is difficult to ascertain in practice because it is both subjective and contextual."[25] The amount of subjectivity in the determination of hostile intent is relative to the amount of one's knowledge of the enemy. Subjectivity reflects assumptions, perspective, and estimations made due to a lack of information.[26] Determination of hostile intent is contextual because the circumstances of the scenario are relevant. In the absence of definitive data and knowledge, commanders must weigh the external factors that feed into the determination of intent: international political climate, immediacy of the threatening act, enemy doctrine, prior enemy actions, etc.

Proportionality, the second necessary element in the use of force, is only of issue if necessity has been determined. Proportionality for self-defense is defined in SROE as:

> Force used to counter a hostile act or demonstrated hostile intent must be reasonable in intensity, duration, and magnitude to the perceived or demonstrated threat based on all facts known to the commander at the time.[27]

The principle of proportionality holds that "self-defense not only has a start point, it has an end point as well."[28] The neutralization or elimination of an adversary's hostile act, or intent, eliminates the justification of self-defense.

Proportionality determines the extent of force, but not necessarily the means. SROE outlines scaled options, ranging from "attempt to de-escalate the situation" (including warning a hostile force) to "attack to disable or destroy," which serves to guide, but not dictate, the use of proportional force.[29] Under U.S. interpretation of international law, as reflected in current SROE, "attack to disable or destroy" is only appropriate "when such action is the only prudent means by which a hostile act or demonstration of hostile intent can be prevented or terminated."[30] However, SROE also states that if self-defense is necessary, "a commander has the authority and obligation to use *all necessary means available* [emphasis added] and to take all appropriate actions to defend that commander's unit and other U.S. forces in the vicinity from a hostile act or demonstration of hostile intent."[31]

Lastly, SROE defines who is responsible for authorizing the use of force in self-defense. Towards what or whom the adversary has initiated the hostile act or demonstrated the hostile intent, defines the level of self-defense and thus, with whom authority for response lies.[32] There are four levels of self-defense defined in SROE: national, collective, unit, and individual. In general terms, national and collective self-defense require NCA determination. Unit level self-defense is "the act of defending a particular U.S. force element, including individual personnel thereof, and other U.S. forces in the vicinity, against a hostile act or demonstrated hostile intent."[33] Individual self-defense is "the right to use all necessary means available and to take all appropriate actions to defend oneself [e.g., above and beyond the constraints of mission ROE] and U.S. forces in one's vicinity from a hostile act or demonstrated hostile intent."[34]

Though authorization for the use of force may be restricted by higher authority under given mission ROE, "a commander has the authority and obligation to use all necessary

means available and to take all appropriate actions to defend that commander's unit and other U.S. forces in the vicinity from a hostile act or demonstration of hostile intent."[35] SROE empowers the commander, or individual, to determine necessity for the use of force in their immediate situation, at the obvious and understood risk to policy (and mission) objectives.

Today's forces under Standing Rules of Engagement. While authority, responsibility, and obligation for self-defense are provided via SROE, determining necessity via hostile intent is excruciatingly subjective, but necessary for maintaining the initiative. Actions—or inactions—can have dire consequences for the individual or unit, as well as the nation (legally and politically), as the international community and American public review the circumstances with 20/20 hindsight. While responsibility and obligation for a time-critical, subjective decision lies with the commander, "it is the international community, and not the States involved in a self-defense action, that decides on the legality of self-defense; the conditions for the exercise of the right of self-defense, collective and individual, are imposed by international law; the international community, acting through the competent organs of the United Nations, passes a judgment on whether the action taken is necessary and proportionate."[36] The strategic implications of the determination for the use of force in self-defense are well highlighted by this perspective. The difficulties and consequences of improperly determining and acting upon hostile intent are contrastingly, but vividly exemplified by the Iraqi Exocet missile attack on USS *Stark* in 1987 and the USS *Vincennes* shoot-down of an Iranian civilian airliner in 1988. Each of these cases demonstrates the contention between certainty in determination and preservation of initiative in decisions of self-defense.

One limitation for present U.S. forces under current SROE is the inability to definitively determine and react to the enemy's "first salvo" in situations of self-defense. SROE has been criticized for failing to provide quantitative measures for such determinations.[37] However, given the current limitations in developing battlespace awareness, the inherent strength of SROE is its lack of specificity, allowing it to be supplemented and applied to any potential combat situation without unintended constraints on a commander's ability for self-defense. The determination of hostile intent in self-defense is specifically left to the subjective judgment of the commander (or the individual, in individual self-defense) in order to allow for "first-hand" interpretation of the scenario. While the broad definitions of hostile intent and the determination of necessity in SROE are deliberate—providing a single rule set applicable to all situations—its lack of explicit measures is perceived as vulnerability.[38]

Network-centric warfare's capabilities. The speed of command that network-centric warfare provides will allow U.S. forces, among other things, to capitalize on information superiority, maneuver, and precision effects "to such an extent to render an adversary effectively paralyzed, 'locked out' of the battle."[39] Indeed, NCW's ability to obtain dominant battlespace knowledge will allow unprecedented initiative for U.S. forces.[40] Though the capabilities of NCW are largely conceptual at this point,[41] war gaming, fleet experiments, and prototypical systems such as Fleet Battle Experiment India[42] and Global 2000[43] are incrementally proving the feasibility of these theories. Information superiority gained by friendly forces in Global 2000 consistently availed militarily feasible opportunities for pre-emptive attack.[44] NCW drastically reduced the "fog of war" providing unprecedented "visibility" of enemy actions and disposition—replacing assumptions with facts.

The capability of NCW to effectively determine and react to the enemy's first salvo will be specifically attributable to the implemented command and control structure. In general, NCW aspires to a "flattened" command and control structure in order to increase efficiency by removing unnecessary "echelons of authority."[45] Information superiority and communication connectivity serve as key enablers for command, allowing control of execution—with clearly conveyed commander's intent—to be delegated to the lowest tactical level.[46] Operational and tactical level commanders will maintain "real-time coordination and assessment, independent of physical separation."[47]

Central to the formation of operational understanding and situational awareness in the NCW command structure is the coordination and presentation of shared knowledge and common information.[48] While the goal in NCW is to distribute control for operational execution to the lowest tactical level, its structure and omnipotent awareness may have reciprocal implications:

> Increased communications capabilities and shared situational awareness will make it possible for senior leaders to direct tactical actions…. Tactical commanders may no longer have the best picture of the battlespace, and with greater situational awareness all around, seniors may be able to help subordinates in the field avoid situations such as the loss of American lives in Somalia or the accidental bombing of the Chinese embassy in Belgrade in 1999.[49]

NCW's connectivity, data processing, and display capability will allow operational commanders to consider more information, effectively increasing their span of control.[50] "If the tempo of the battlefield permits, or if the sensitivity or importance of a particular aspect of the conflict warrants the commander's personal attention, a commander would have the ability to manage at a micro level as well."[51]

The advantages of increasing awareness and connectivity throughout the command structure are immense—including flexibility of options, real-time planning, increased unity of command and effort, etc. However, Thomas Barnett's observation illustrates the potential unintended consequences of this capability:

> "NCW promises to flatten hierarchies, but the grave nature of military operations may push too many commanders into becoming control freaks, fed by an almost unlimited data flow."[52]

In contrast, Richard Harknet's view shows a second perspective of potential outcomes in NCW's command structure:

> The leveling of traditional hierarchical structure also creates the converse danger of macro-management: the temptation of actors in the field to make decisions that should be made by higher authorities. Giving the troops a "god's–eye view" through direct access to satellites and other remote sensors may encourage them to act independently.[53]

The two opposing outlooks present a single question: With whom will the responsibility and authority for authorizing force in unit self-defense reside in NCW? This question is complicated by the fact that NCW theories envision two distinct command and control structures. VADM Aurthur Cebrowski envisions a bottom-up structure, utilizing distributed decision-making, capable of real-time adaptation to form temporary mission-specific fighting organizations when necessary.[54] Admiral William Owens sees NCW as a "system of systems," executed under "an explicit control mechanism to prevent operational and tactical execution errors."[55] The two theories for NCW command and control are diametrically opposed: Vice Admiral Cebrowski envisioning a self-organized, de-centralized system and Admiral Owens envisioning a highly organized, central system.

Under the Admiral Owens' NCW concept of "system of systems", the actual division between tactical (TACON) and operational control (OPCON) of forces could erode as

operational commanders utilize the real-time awareness of a common operating picture to direct or re-direct forces.[56] His theory of common operating picture for reducing the fog of war has several implications for self-defense within current SROE.

Automated determination. The "system of systems" concept of command and control envisions automation of weapon and firing systems through a decision-data network that provides hostile determination and discrimination based on pre-established commander's intent, ROE, and established doctrine.[57] While this system may be feasible with well-defined mission accomplishment ROE in conventional warfare, its feasibility is questionable throughout the full spectrum of combat and combat systems. More specifically, the "system of systems" command and control structure, while attempting to eliminate ambiguity and subjectivity through the automated determination of hostile intent, may be detrimental to policy and inconsistent with law in authorizing force for self-defense. Furthermore, the omnipotent nature of this command structure may increase the vulnerability of forces by creating "decision paralysis" among subordinate commanders.

The implementation of an automated "if-then" decision matrix will require quantitative measurement of factors for determining hostile intent via provided information superiority with "trip-wire" algorithms.[58] Computer data processing and automated weapon control functions will provide extreme speed of command, therefore effectively conserving and utilizing time for improving the certainty of hostile determination whilst preserving the ability to respond in advance of an imminent enemy attack.[59] Weapon system automation will provide timely target identification for a network of cooperatively capable sensor-weapon systems to effect immediately decisive results against an adversary.

In reality, regardless of the information fidelity provided by NCW, automated systems cannot account for all of the subjective factors necessary in self-defense. NCW may reduce the fog of war, but it cannot remove the glare that will always be present from human interaction and creativity. [60] Automated ROE cannot factor in the intuitive considerations required for the determination of hostile intent. While common operating picture may display enemy forces as a *threat* (evaluating relative position, capability, and even weapon system status), they cannot definitively determine that an enemy is *threatening* until a hostile act has actually occurred.[61] In order to make a determination of necessity that is congruous with both law and national policy, systems would have to relate own force (net-wide) capabilities to enemy disposition, within the context of the situation. It is the latter part—"within the context of the situation"—that challenges the feasibility of automated determination of hostile intent for authorizing force in self-defense.

Perspective in determination. The very command interaction and common operating picture that ADM Owens' theory of NCW is based on may further complicate the determination for the use of force in self-defense. "Information superiority" and "common operating picture" do not necessarily relate to common perspective. Intuition and cognitive impressions can alter the perspective of information and knowledge, specifically in the determination of subjective or contextual decisions such as hostile intent.

> The problem, simply stated, is that having the same information does not necessarily lead actors to reach the same conclusion about how to respond…. Without a perfect integration of political-military goals throughout the network, without a fusion of perspectives and view, and without the development of new command rule sets that clearly determine who makes decisions, the potential for different actors with the same information to make conflicting choices will surely exist."[62]

NCW's prevalence of information will reduce or eliminate assumptions, but it cannot remove perspective from the decision making process.[63] Experience, responsibility, and expectation all contribute to human intuition, forming different perspectives of a common situation.[64] Under current SROE, such varied perspectives could have significant impact on the determination of hostile intent. The implication is that higher authority could incorrectly influence, or worse dictate, the determination of necessity because of higher objectives, misperceived threats or in response to the tempo of information instead of the immediacy of the situation.[65]

Decision paralysis. As a result of the interactive command relationships in Admiral Owens' theory of NCW, subordinate commanders could be overwhelmed by information and direction, resulting in inaction or indecision during the critical evaluation of necessity.[66] In this situation, NCW's design would allow other commanders to take immediate action to achieve the mission, or in this case, direct the use of force for self-defense of another unit or individual. Is the increased potential for "remote" determination of necessity in self-defense an example of self-synchronization or usurpation of responsibility? The answer depends on whether the inaction by the subordinate was an accurate and deliberate postponement due to the knowledge derived from his unique perspective, or if the inaction was indeed due to task or information saturation.

Opportunity or necessity? In contrast, Vice Admiral Cebrowski's vision of a bottom-up system feeds on the very command by negation that current SROE is written for. NCW will provide superior information and the ability to preempt hostile action. However, the ability to preempt is explicitly limited by the legal definition of necessity and determination of hostile intent. Additionally, commanders must ensure that the use of force

is "the only prudent means by which a hostile act or demonstration of hostile intent can be prevented or terminated."[67] The opportunity of enemy vulnerability does not necessarily afford authority for the use of force under the definition of necessity.

> The ability to take action on a more compressed timeline creates a dynamic of its own. Now that commanders have more timely and accurate information of the enemy they tend to become captivated by the mode of presentation and type of information, that is, video feeds. The urge to act on the information is stronger than before because the fog of war is not as severe.[68]

The theorized—and already realized—operational capabilities of NCW (specifically, information superiority and speed of command) could result in commanders reacting to opportunity vice necessity. However, the reality that information or opportunity—even in NCW—may be fleeting does not negate the constraints of necessity.[69]

At issue is a question of policy durability: though information may provide determination of hostile intent, will U.S. policy allow local commanders to utilize preemptive force in order to "stop something before it starts?"[70] The point is that "much of the operational advantage gained by [NCW] could be thrown away by strategic-level caution, delay or inaction."[71] Current SROE—in the absence of supplemental ROE—would only allow such action with the specific determination of the NCA. This constraint is based on the varied and contrasting appreciations for anticipatory self-defense in the international community.

Defender or aggressor? Regardless of the implemented command and control structure in NCW, the implications of even anticipating the requirement for using force in self-defense may be as significant as the actual use of force. How commanders exercise the options availed to them by early determination via NCW's information dominance could have significant, detrimental legal and political effects under current interpretations of the

U.N. Charter.[72] The preparations for self-defense could well be interpreted as "aggressive" and "threatening" by the very enemy that one is preparing to engage, thus accelerating an inevitably fateful chain of events that would antagonize a hostile act.[73] The mediation of this scenario rests with the legality of the U.S. mission, or presence, in the first place. Nonetheless, this scenario highlights the importance of such considerations for the deployment of U.S. forces. Even when operating with supplemental ROE, this type of scenario—created by increased, but less than complete knowledge—may drive a commander to act in accordance with the right to self-defense and therefore it illustrates the importance for considering all of the unintended situations that new operational capabilities may create.

Summary. Examining future force capabilities through the process of force authorization in self-defense reveals several vulnerabilities and questions for both NCW and SROE. Likewise, it reiterates the fact that advances in operational capability can be significantly constrained, or even undermined, by politics and law if they go unconsidered during research and development.

The command and control structure that evolves with NCW will specifically affect the relevance of current SROE to future capabilities. Automated decision systems and common operating pictures will not eliminate perspective and the requirement for subjective assessment in determining necessity for the use of force in self-defense. The fear of uncertainty in determination will continue to be a reality in NCW. As such, speed of command will continue to be constrained by the requirement for judgments based in empirical, vice quantitative data during determination of necessity in self-defense. Development of NCW's command and control structure and doctrine must appreciate and address the potential for creating ambiguity in identifying responsibility and authority,

particularly under current SROE guidance. "Unit" under current SROE does not clearly translate in NCW, where physical platforms hold less definitional importance than network architectures. Any ambiguity in command is a dangerous vulnerability for U.S. forces.

Future NCW command and control evaluations should include the analysis of its capabilities in the transition from pre-hostilities to hostilities under SROE, absent supplements, to determine the durability of the current self-defense guidance and to identify ambiguities in responsibilities and authority. Evaluation must determine—based on the implemented command structure—the mechanism or process which will ensure that strategic and operational commanders are restrained from directing tactical actions (specifically in self-defense) that conflict with the observations and analysis of "on-scene" tactical commanders. The evaluation should also identify the process or method for identifying and "pushing" priority information from the strategic or operational commander to the tactical commander in order to enhance, but not saturate, his decision-making process. Additionally, feedback mechanisms may be required to provide higher commanders with confidence in subordinate unit awareness and intentions.

Automated determination of hostile intent and weapon control will not be applicable throughout the full spectrum of warfare. In fact, in situations unmodified by supplemental ROE, automated determination systems are inadequate for providing force protection without likely adverse affect to national policy and possible legal implications. Without extensive real-time insertion of contextual factors (and those being subject to perspective), NCW will be no more able to classify hostile intention via "if-then wickets" than today's systems. However, automated determination and weapons system control will be a key enabler when guided by the tangible factors in mission accomplishment ROE.

Recommendations. First, *automated decision and weapon systems in NCW should continue to be evaluated via further gaming and exercises to establish value, faults, and limitations in contributing to determination and response in self-defense situations*. Further study should examine the capability for acquiring adequate data and information that will contribute to an earlier decision of hostile intent, including the determination of specific nodes, characteristics, or elements for sensor observation. War gaming can reveal how information prioritization and analysis from collection to distribution develops user perspectives via a common operating picture. Measures of effectiveness in the analysis should differentiate false positives (incorrect determinations of hostile courses of action), from correct determinations, and from indiscernible threat actions (ambiguous determinations).

While increased battlespace knowledge in NCW may change the perception of necessity, the legal definition and the circumstances justifying the use of force currently remain the same. Therefore, *the theorized desire to act on information superiority and speed of command, possibly prior to the determination of legal necessity in self-defense, must be examined further.* If not addressed, this potential will significantly undermine U.S. policy and have legal implications, as such use of force could be categorized in international opinion as "aggression," vice "self-defense."

Commanders must realize that the future effects of network-centric warfare may eventually form new precedence for the interpretation of necessity in international law (much as the advent of nuclear weapons did with regard to proportionality). Until such precedence is established, early anticipatory actions in network-centric warfare, if unchecked, will significantly strain national policy and current international law.

Further, *the opportunity to act on the tempo of operations and the fidelity of information, vice necessity, in justifying force under the concept of anticipatory self-defense should be investigated via observation in war gaming.* Further empirical data on this subject will be key to developing proper command and control doctrine in NCW. Products of this evaluation should include a method or concept for quantifying and displaying the time-space advantage of a particular situation for the commander's consideration in his decision-reaction process. (A current-generation example of this is the concept utilized by U.S. fighter aircrews for determining their time-distance (space) relationship to an adversary.[74])

In the absence of the identification and further development of NCW's specific command and control structure and an examination of its execution from pre-hostility to hostility phase of combat, *no recommendations can be made for the revision of current SROE.* In fact, the broad subjectivity of existing SROE cannot be eliminated due to the real potential for autonomous deployment—such as individual ground forces or non-networked units—even within a network-centric force structure.

Lastly, this examination identifies the requirement for further legal and political determination of which assets, threatened by hostile intent or action, may be used for the justification of force in self-defense. NCW will employ expeditionary sensor grids (ESG) and unmanned vehicles that will not only enhance battlespace knowledge, but will be central to U.S. military capability. *How an "attack" on these assets or on U.S. C4ISR[*] systems figure into operational planning and the commander's determination of necessity in utilizing force for self-defense demands further study.*

---

[*] Command, control, communications, computers, intelligence, surveillance, reconnaissance, (and information operations support).

Conclusion. Network-centric warfare offers the opportunity for U.S. force structure to develop around a concept that yields decisive battlespace advantage. However, the realization of this advantage is contingent on the cohesive relationship between technological capability, doctrine, policy, and law. *Standing Rules of Engagement for U.S. Forces* provides the baseline guidance for the use of force in all U.S. military missions. Consistency must be maintained between this guidance and force capability to ensure that military efforts and actions continue to be effective levers of national power.

NOTES

[1] Joint Chiefs of Staff, *Joint Vision 2020* (Washington, D.C.: U.S. Government Printing Office, June 2000), 3; *Joint Electronic Library* [CD-ROM] (Washington, D.C.: Joint Chiefs of Staff, September 1996).

[2] Dominant battlespace knowledge: the ability to see, understand, and effectively act. This term describes the ability to capitalize on information superiority. For detailed information, see: Stuart E. Johnson and Martin C. Libicki, eds., *Dominant Battlespace Knowledge*, rev. ed. (Washington, DC: National Defense University, 1996).

[3] Joint Chiefs of Staff, *Standing Rules of Engagement for U.S. Forces*, CJCSI 3121.01A (Washington, D.C.: January 2000).

[4] Cebrowski, Arthur K., "President's Forum," *Naval War College Review*, 54, no. 2 (Spring 2001): 11.

[5] Cebrowski, Arthur K., and John J. Garstka, "Network-Centric Warfare—Its Origin and Future," *U.S. Naval Institute Proceedings*, 124, no. 1 (January 1998): 32.

[6] Duncan, James C., "The Commander's Role in Developing Rules of Engagement," *Naval War College Review*, 52, no. 3 (Summer 1999): 79-80.

[7] Schmidt, Michael N., ed., *International Law Studies: Levie on the Law of War* (Newport, RI: U.S. Naval War College Press, 1998), 246. CJCS Joint Pub 1-02 and CJCSI 3121.01A offer similar definitions, though they replace "National Command Authorities" with "competent military authority." The CJCS definitions reflect the mechanism for issuing ROE supplemental, which may—in prescribed circumstances—be issued by commanders subordinate to the NCA. Schmidt's definition was used to reflect the direct interest and authority of the NCA, specifically in SROE—the interest of this paper.

[8] Duncan, 79-80.

[9] Specifically Law of Armed Conflict, The Charter of the United Nations, and U.S. treaties. Under U.N. Charter, the use of force is legal under only two conditions: (1) self-defense—a prescribed in Article 51, (2) U.N. approved coercive use of force—under Article 39. Otherwise, Article 2(4) specifically prohibits the use or *threat* of force. For further explanation see: Charter of the United Nations; Stanimir A. Alexandrov, *Self-Defense Against the Use of Force in International Law* (The Hague, The Netherlands: Kluwer Law International, 1996); Horace B. Robertson, "Contemporary International Law Relevant to Today's World?" *Naval War College Review*, 45, no. 3 (Summer 1992): 89-103.

[10] David E. Graham, editorial review of "Deadly Force *Is* Authorized," by W. Hays Parks, *U.S. Naval Institute Proceedings*, 127, no. 5 (May 2001): 14.

[11] Joint Chiefs of Staff, *Standing Rules of Engagement for U.S. Forces*, 2.

[12] Ibid.

[13] Schmidt, 251-252.

[14] Joint Chiefs of Staff, *Standing Rules of Engagement for U.S. Forces*, A-5.

[15] Schmidt, 252.

[16] Department of the Navy, *The Commander's Handbook on the Law of Naval Operations*, NWP 1-14M (Washington D.C.: October 1995), 4-3.

[17] Joint Chiefs of Staff, *Standing Rules of Engagement for U.S. Forces*, A-5.

[18] Ibid.

[19] Alexandrov, 95-100.

[20] Schmitt, 253.

[21] Joint Chiefs of Staff, *Standing Rules of Engagement for U.S. Forces*, A-5.

[22] Alexandrov, 149.

[23] For excellent international perspectives on the legitimacy of anticipatory self-defense, see Stanimir A. Alexandrov, *Self-Defense Against the Use of Force in International Law*, (The Hague, The Netherlands: Kluwer Law International, 1996) and Yoram Dinstein, *War, Aggression, and Self-Defense*, 2nd ed. (Cambridge, England: Cambridge University Press, 1994).

[24] Alexandrov, 100.

[25] Schmitt, 254.

[26] Ibid., 254.

[27] Joint Chiefs of Staff, *Standing Rules of Engagement for U.S. Forces*, A-5.

[28] Schmitt, 257.

[29] Joint Chiefs of Staff, *Standing Rules of Engagement for U.S. Forces*, A-6.

[30] Ibid.

[31] Ibid., A-3.

[32] Ibid., A-3–A-4.

[33] Ibid., A-4.

[34] Ibid., A-5.

[35] Ibid., A-3. Additionally, this point is emphasized in bold print, no less than eleven times throughout the document.

[36] Alexandrov, 296.

[37] Parks, W. Hays. "Deadly Force *Is* Authorized." *U.S. Naval Institute Proceedings*, 127, no. 1 (January 2001): 33.

[38] Parks, 36-37.

[39] Watman, Kenneth, "Global 2000," *Naval War College Review*, 2 (Spring 2001): 76.

[40] Johnson and Libicki, 43.

[41] Watman, 76

[42] Naval War College Faculty, comp. & ed., *Fleet Battle Experiment India* (Newport, RI: U.S. Naval War College, 2001). Fleet Battle Experiment India was conducted 18-28 June 2001 by the Maritime Battle Center (MBC) Department of the Naval Warfare Development Command (NWDC) in Newport, RI. Information herein was derived from the aforementioned unclassified overview. Further information is available via NWDC's SIPRnet website: http://www.nwdc.navy.smil.mil.

[43] Global 2000 was a war game conducted 14-25 August 2000 by the War Gaming Department of the Naval Warfare Development Command (NWDC) in Newport, RI. Information herein was derived from Kenneth Watman, "Global 2000," *Naval War College Review*, 2 (Spring 2001): 75-88.

[44] Watman, 83.

[45] Leonhard, Robert R., *The Principles of War for the Information Age* (Novato, CA: Presidio, 1998), 199.

[46] Leonhard, 201.

[47] Naval War College Faculty, *Network Centric Operations: A Capstone Concept for Naval Operations in the Information Age*, smooth draft (Newport, RI: U.S. Naval War College, 2000), 9.

[48] Ibid.

[49] Dahl, Erik J., *Network Centric Warfare and the Death of Operational Art* (Newport, RI: U.S. Naval War College, 2001), 10-11.

[50] Leonhard, 199.

[51] Johnson and Libicki, 86.

[52] Barnett, Thomas P. M. "The Seven Deadly Sins of Network-Centric Warfare." *U.S. Naval Institute Proceedings*, 125, no. 1 (January 1999): 31.

[53] Harknet, Richard J.. "The Risks of a Networked Military." *Orbis* (Winter 2000): 135.

[54] Geron, Michael Craig, *Commander's Intent: The Critical Transformation Challenge for Networked Forces* (Newport, RI: U.S. Naval War College, 2001), 2.

[55] Ibid.

[56] Ibid.

[57] Ibid., 6.

[58] Johnson and Libicki, 59.

[59] Ibid., 120.

[60] The technical realities are addressed in: Johnson and Libicki, 68. The theoretical views of this are described in: Carl von Clausewitz, *On War*, edited and trans. by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 156.

[61] Schmitt, 254. The distinction of threat and threatening is that of capability and intention.

[62] Harknet, 136.

[63] Barnett, 30-31.

[64] Lee, James D., *Information Dominance in Military Decision Making* (Fort Leavenworth, Kansas: Army Command and General Staff College, 1999), 85.

[65] Barnett, 29-30.

[66] Brad Nelson, "Applying the Principles of War in Information Operations," Military Review, 78, no. 5 (September-November 1998): 31; quoted in James D. Lee, *Information Dominance in Military Decision Making* (Fort Leavenworth, Kansas: Army Command and General Staff College, 1999), 27.

[67] Joint Chiefs of Staff, *Standing Rules of Engagement for U.S. Forces*, A-6.

[68] Lee, 53.

[69] Watman, 83.

[70] Ibid., 83-84.

[71] Ibid., 84.

[72] Alexandrov, 111-112.

[73] Ibid., 112. According to Alexandrov, "aggression" is actually defined as the "first use of armed force," not the threat to use force. However, in this example the impression and perception are more important than the legal definition.

[74] Fighter aircrews utilize weapon-platform comparisons to develop "rules of thumb" for quantifying available reaction times, and thus for formulating options. Further information is available from Navy Fighter Weapons School, *TOPGUN Manual* (NAS Fallon, NV: Navy Fighter Weapons School, 2001), chapter. 37.

BIBLIOGRAPHY

Alberts, David S., John J. Garstka, Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. rev. Vienna, VA: Department of Defense, C4ISR Cooperative Research Program, 1999.

Alexandrov, Stanimir A. *Self-Defense Against the Use of Force in International Law*. The Hague, The Netherlands: Kluwer Law International, 1996.

Barron, Michael J. *Operational Level Command: Who is in Charge?* Fort Leavenworth, KS: U.S. Army and General Staff College, School of Advanced Military Studies, 1988.

Barnett, Thomas P. M. "The Seven Deadly Sins of Network-Centric Warfare." *U.S. Naval Institute Proceedings*. 125, no. 1 (January 1999): 28-31.

Becker, Patrick J. *What is an Adequate Decision Support System for the Operational Level of War?* Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, 1989.

Bowdish, Randall G. Review of *Network Centric Warfare: Developing and Leveraging Information Superiority*, by David S. Alberts, John J. Garstka, Frederick P. Stein. *U.S. Naval Institute Proceedings*. 125, no. 12 (December 1999): 78-82.

Burton, Michael A. *Rules of Engagement: What is the Relationship Between Rules of Engagement and the Design of Operations?* Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, 1987.

Cebrowski, Arthur K., and John J. Garstka. "Network-Centric Warfare—Its Origin and Future." *U.S. Naval Institute Proceedings*. 124, no. 1 (January 1998): 28-35.

Cebrowski, Arthur K.. "President's Forum." *Naval War College Review*, 54, no. 2 (Spring 2001): 4-11.

Charter of the United Nations.

Dahl, Erik J. *Network Centric Warfare and the Death of Operational Art*. Newport, RI: U.S. Naval War College, 2001.

Dinstein, Yoram. *War, Aggression, and Self-Defense*, 2nd ed. Cambridge, England: Cambridge University Press, 1994.

Duncan, James C. "The Commander's Role in Developing Rules of Engagement." *Naval War College Review*. 52, no. 3 (Summer 1999): 76-89.

Geron, Craig. *Commander's Intent: The Critical Transformation Challenge for Networked Forces*. Newport, RI: U.S. Naval War College, 2001.

Graham, David E. Editorial review of "Deadly Force *Is* Authorized," by W. Hays Parks. *U.S. Naval Institute Proceedings*, 127, no. 5 (May 2001): 12-18.

Harknet, Richard J. "The Risks of a Networked Military." 44, no. 1 *Orbis* (Winter 2000): 127-143.

Henseler, Sean P. *Addressing the Legal Challenges of Network Centric Warfare—Case in Point: The Legal Implications of Obtaining an "Information and Knowledge Advantage" Prior to Hostilities.* Newport, RI: U.S. Naval War College, 2001.

Hutcherson, Norman B. *Command & Control Warfare: Putting Another Tool in the Warfighter's Data Base*. Maxwell , AL: U.S. Air University Press, 1994.

Johnson, Stuart E. and Martin C. Libicki, eds. *Dominant Battlespace Knowledge*, rev. ed.. Washington, DC: National Defense University, 1996.

Kamradt, Henry D. and Douglas H. L. MacDonald. *The Implications of Network Centric Warfare for U.S. and Multinational Military Operations*. Newport, RI: Strategic Research Dept., Center for Naval Warfare Studies, U.S. Naval War College, 1998.

Khalizad, Zalmay M. and White, John P., eds. *Strategic Appraisal. The Changing Role of Information in Warfare.* Santa Monica, CA: RAND Corporation, 1999.

Lee, James D. *Information Dominance in Military Decision Making*. Fort Leavenworth, KS: U.S. Army Command and General Staff College, 1999.

Leonhard, Robert R. *The Principles of War for the Information Age*. Novato, CA: Presidio, 1998.

Nelson, Brad. "Applying the Principles of War in Information Operations." Military Review, 78, no. 5 (September-November 1998): 31. Quoted in James D. Lee, *Information Dominance in Military Decision Making* 27. Fort Leavenworth, Kansas: Army Command and General Staff College, 1999.

Parks, W. Hays. "Deadly Force *Is* Authorized." *U.S. Naval Institute Proceedings*, 127, no. 1 (January 2001): 32-37.

Robertson, Horace B. "Contemporary International Law Relevant to Today's World?" *Naval War College Review*, 45, no. 3 (Summer 1992): 89-103.

Scarborough, Sheila, "Network-Centric Warfare: Is It Worth the Risk?" *U.S. Naval Institute Proceedings*. 127, no. 5 (May 2001): 30-33.

Schmitt, Michael N., ed. *International Law Studies: Levie on the Law of War*. Newport, RI: U.S. Naval War College Press, 1998.

U.S. Department of the Navy. *The Commander's Handbook on the Law of Naval Operations*. NWP 1-14M. Washington D.C.: October 1995.

U.S. Joint Chiefs of Staff. *Joint Vision 2020*. Washington, D.C.: U.S. Government Printing Office, June 2000. Available on *Joint Electronic Library* [CD-ROM]. Washington, D.C.: Joint Chiefs of Staff, September 1996.

_____. *Standing Rules of Engagement for U.S. Forces*. CJCSI 3121.01A. Washington, D.C.: January 2000.

U.S. Naval War College Faculty, comp. & ed. *Fleet Battle Experiment India*. Newport, RI: U.S. Naval War College, 2001.

_____. *Network Centric Operations: A Capstone Concept for Naval Operations in the Information Age*, smooth draft. Newport, RI: U.S. Naval War College, 2000.

U.S. Navy Department. *The Commander's Handbook on the Law of Naval Operations*. Naval Warfare Publication 1-14M. Norfolk, VA: 1995.

U.S. Navy Fighter Weapons School. *TOPGUN Manual*. NAS Fallon, NV: Navy Fighter Weapons School, 2001.

von Clausewitz, Carl. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Watman, Kenneth. "Global 2000." *Naval War College Review*, 54, no. 2 (Spring 2001): 75-88.